DUBAI INTERNATIONAL ACADEMY

Al Barsha

Dream. Inspire. Achieve. *Belong*

E-SAFETY
POLICY

Last updated: September 2023
Next Review: August 2024

CONTENTS

Dream. Inspire. Achieve. *Belong*

1 Rationale

DIAB is committed to an innovative learning environment providing access to technology to support students to become self-directed, collaborative learners. The application of digital technologies supports Teaching & Learning, enriching student learning through internal & external online resources. DIAB aims to support best practice to maintain, develop and promote safer practices. The aim is to protect users from potentially harmful content or activities, such as grooming, pornography, cyber bullying, etc and includes both websites and apps.

2 Definitions

E-safety refers to keeping users safe while using electronic devices and accessing material, such as the internet. Inappropriate Content is that considered unsuitable or harmful to students such as material that is racist, sexist, inflammatory, threatening, pornographic, hateful, obscene or abusive in nature, promotes or encourages illegal activities or violence.

3 Expectations & Responsibilities

3.1 School will:
- Ensure appropriate training, lessons and workshops for staff, students and parents, including but not limited to, Academic Integrity Policy, Cyber-Bullying and Online Safety
- Ensure the school's technical infrastructure is secure, not open to misuse and remains up-to-date with potential threats.
- Ensure all elements of the school network, mobile devices, etc are monitored for any misuse, reporting concerns to the Senior Leadership Team
- Ensure the E-Safety and Acceptable Use Policy (AUP) is read, understood and followed by all parties
- E-safety issues are embedded in all aspects of the curriculum, events and activities, such as Safer Internet Day.
- Ensure that all online resources used in lessons, are pre-checked as suitable for their use, without any unsuitable material
- Not share personal data and will ensure all such data or information is held securely

3.2 Students will:
- Be responsible for using the school digital technology systems in accordance with the Student Acceptable Use Policy on all devices
- Understand and follow the Academic Integrity Policy
- Not take images or videos of others without consent or that is not for school purposes
- Not share inappropriate material through any format
- Report abuse, misuse or access to inappropriate materials to Senior Leaders

- Not engage in inappropriate comments about the school, staff or students via social media

3.3 Parents will:
- Support school policies and decisions relating to e-safety, including engaging with school workshops related to e-safety
- Support their children to understand the Acceptable Use Policy.
- Not take images or videos of others without consent or that is not for school purposes
- Only accept information from official school sources
- Not engage in inappropriate comments about the school, staff or students via social media

4 Acceptable Use Policy

DIAB operates a BYOD policy and students will be required to adhere strictly to the rules for BYOD usage and understand the consequences of not following these rules.

- Members of staff may access a child's device at any time if they feel it is being misused.
- Devices can be used only in the classroom as a learning tool under direction of the teacher.
- Devices are not allowed outside the classroom in the corridors, playgrounds, cafes or toilets unless directed to by a member of staff.
- Devices may be used on the school transport system by students from Grade 6, but only with headphones attached.
- Students may not record, transmit or post photographic images or video of a person, or persons without their permission.
- Students must not engage in cyberbullying, harassment, or disrespectful conduct toward others, staff or students.
- Students must not use language online that would be unacceptable in school.
- Parents must not contact children on their device during school hours. Parents can contact through school reception and/or appropriate email channels.
- IT has the right to collect and inspect any device that is suspected of being the source of an attack or virus infection.
- Students may only access files on the computer or internet sites which are relevant to classroom curriculum.
- Students must ensure that the private content and media stored on the device is not used during school time.
- Students must report security or network problems to a teacher or administrator.
- In using the network and internet, users should not reveal personal information such as a home address or telephone number.
- Printing from a student's personal device may not be possible at school.

- Devices must be charged prior to bringing it to school and run off its own battery while at school. Limited charging resources will be available in school, but this is not guaranteed.
- Students are not permitted to use a VPN or Mobile Data onsite

5 Further Reading

www.nationalonlinesafety.com
http://www.bbc.co.uk/cbbc/topics/stay-safe
http://www.bbc.co.uk/cbeebies/grownups/help/internet-use-and-safety
https://www.commonsensemedia.org
http://www.kidsmart.org.uk/beingsmart